

# UNIFORMLY COUNTING RATIONAL POINTS ON CONICS

EFTHYMIOS SOFOS

ABSTRACT. We provide an asymptotic estimate for the number of rational points of bounded height on a non-singular conic over  $\mathbb{Q}$ . The estimate is uniform in the coefficients of the underlying quadratic form.

## 1. INTRODUCTION

Let  $Q(\mathbf{x}) \in \mathbb{Z}[x_1, x_2, x_3]$  be a non-singular quadratic form. We denote by  $\mathbb{Z}_{\text{prim}}^3$  the integer vectors  $\mathbf{x}$  that are primitive, i.e. that satisfy  $\gcd(\mathbf{x}) = 1$ . Our main concern in this paper regards the number of primitive integer zeros of  $Q$  contained on an expanding region of  $\mathbb{R}^3$ . It is therefore only the case that  $Q$  is isotropic that we are interested in and we will proceed under this assumption for the rest of the paper.

For any arbitrary norm  $\|\cdot\| : \mathbb{R}^3 \rightarrow \mathbb{R}_{\geq 0}$  define the counting function

$$N(Q, B) := \#\{\mathbf{x} \in \mathbb{Z}_{\text{prim}}^3 : Q(\mathbf{x}) = 0, \|\mathbf{x}\| \leq B\}.$$

A very special case of the work [FMT89] establishes the asymptotic formula

$$N(Q, B) \sim c_Q B,$$

valid for  $B \rightarrow \infty$ . This confirms the Manin conjecture and furthermore  $c_Q = c_Q(\|\cdot\|)$  is the constant predicted in [Pey95].

Let  $\langle Q \rangle$  stand for the maximum modulus of the coefficients of  $Q$ . As pointed out in [BVV12], one expects the existence of absolute constants  $\gamma, \delta > 0$ , such that

$$(1.1) \quad N(Q, B) = c_Q B + O(B^{1-\delta} \langle Q \rangle^\gamma).$$

Our aim to establish such an estimate and furthermore to state explicitly admissible values for  $\gamma$  and  $\delta$ .

We begin by recalling existing results related to this subject. Let  $w : \mathbb{R}^3 \rightarrow \mathbb{R}_{\geq 0}$  be a smooth weight function of compact support and let

$$N_w(Q, B) := \sum_{\substack{\mathbf{x} \in \mathbb{Z}_{\text{prim}}^3 \\ Q(\mathbf{x})=0}} w(B^{-1}\mathbf{x}).$$

---

*Date:* May 3, 2013.

*2010 Mathematics Subject Classification.* 11D45 (14G05).

It is proved in [HB96, Cor.2] that there exists a positive constant  $c_1$  such that one has

$$N_w(Q, B) = c_{Q,w}B + O_{Q,w}(B \exp\{-c_1\sqrt{\log B}\}),$$

as  $B \rightarrow \infty$ . The proof is done via a modification of the circle method.

Let  $\Delta_Q$  and  $\Delta_0$  be the discriminant and the greatest common divisor of the  $2 \times 2$  minors of the matrix of the form  $Q$ , respectively. In [BHB05, Cor. 2], it is proved that

$$N(Q, B) \ll \tau(|\Delta|) \left( 1 + \frac{B\Delta_0^{1/2}}{|\Delta|^{1/3}} \right),$$

where  $\tau$  denotes the divisor function. It should be stressed that the implied constant is absolute.

We provide the definition of the leading constant  $c_Q$  before stating our main result. We define the Hardy–Littlewood local densities following [HB96]. Let

$$(1.2) \quad \sigma_\infty := \sigma_\infty(Q, \|\cdot\|) = \lim_{\epsilon \rightarrow 0} \frac{1}{2\epsilon} \int_{\substack{|Q(\mathbf{x})| \leq \epsilon \\ \|\mathbf{x}\| \leq 1}} 1 \, d\mathbf{x},$$

and similarly for any prime  $p$ , let

$$(1.3) \quad \sigma_p := \sigma_p(Q) = \lim_{n \rightarrow \infty} \frac{1}{p^{2n}} N^*(p^n),$$

where for any positive integer  $n$ ,

$$N^*(p^n) := \#\{\mathbf{x} \pmod{p^n} : p \nmid \mathbf{x}, Q(\mathbf{x}) \equiv 0 \pmod{p^n}\}.$$

The Peyre constant is then defined as

$$(1.4) \quad c_Q = \frac{1}{2} \sigma_\infty \prod_p \sigma_p$$

where the product is taken over the set of primes. Let  $C \subseteq \mathbb{P}^2$  be the smooth projective curve defined by  $Q$ . The existence of the factor  $\frac{1}{2}$  is due to the fact that  $\text{Pic}(C) \cong \mathbb{Z}$ , which implies that  $\alpha(C) = \frac{1}{2}$ , where  $\alpha(C)$  is the volume of a certain polytope contained in the cone of effective divisors.

Next, let

$$(1.5) \quad K_0 := 1 + \sup_{\mathbf{x} \neq \mathbf{0}} \frac{\|\mathbf{x}\|_\infty}{\|\mathbf{x}\|},$$

where  $\|\cdot\|_\infty$  is the usual supremum norm. Notice that  $K_0$  is a constant depending only on the choice of norm  $\|\cdot\|$ . We have the following result.

**Theorem 1.** *Let  $Q$  be a ternary non-singular integer quadratic form with a rational zero. Then*

$$N(Q, B) = c_Q B + O\left((BK_0)^{\frac{1}{2}} (\log BK_0) \langle Q \rangle^6\right),$$

for  $B \geq 2$ . The implied constant in the estimate is absolute.

The proof of Theorem 1 reveals that at the expense of an implied constant that depends on  $\gamma$ , one can replace the exponent 6 by any  $\gamma > \frac{11}{2}$ . Further improvements may follow using [Hoo68, Theorem 1]. We hope it will be apparent to the reader that the main value of Theorem 1 lies in the general class of curves to which the result applies, rather than the exponent obtained.

The proof of Theorem 1 is conducted in two stages. Firstly, in §2–§6, we prove Theorem 1 for conics of a special shape, using the fact that since  $C(\mathbb{Q}) \neq \emptyset$ , there is a morphism  $\mathbb{P}^1 \rightarrow C$ . The conditions involving the resulting parametrising functions lead to a lattice counting problem. One should comment that the choice of the parametrising functions is not unique and that choosing them appropriately plays a significant rôle. An amount of work regarding this issue has taken place, as the papers [CR03] and [Sim06] reveal. The second stage is performed in §7. Here we apply a unimodular transformation to a conic of general shape to transform the problem into the one we have already treated.

**Notation.** The implied constants in the  $O(\cdot)$  notation will be absolute throughout this paper, except where specifically indicated, via the use of a subscript. The norm notation  $\|\cdot\|$  will be reserved for norms of elements of  $\mathbb{R}^3$  while  $\|\cdot\|_\infty$  will be used for the supremum norm of matrices as well as the supremum norm of  $\mathbb{R}^3$ . We denote the generalised divisor function by  $\tau_k(n)$ , which is defined to be the number of representations of  $n$  as the product of  $k$  natural numbers. The well-known bound  $\tau_k(n) \ll_{k,\epsilon} n^\epsilon$ , valid for each  $\epsilon > 0$ , shall be used. By  $\sum_{(s,t) \pmod n}^*$ , we shall mean a summation for  $s, t \in [1, n]$ , subject to the condition  $\gcd(s, t, n) = 1$ .

## 2. PRELIMINARY ESTIMATES

Throughout §2–§6, we denote by  $Q$  the quadratic form of the special shape,

$$Q(\mathbf{x}) = ax^2 + bxy + dxz + eyz + fz^2,$$

where  $a, \dots, f \in \mathbb{Z}$ . We will denote by  $\Delta_Q$  its discriminant,

$$\Delta_Q = ae^2 + fb^2 - bde.$$

It is our intention in the aforementioned sections to prove the following special version of Theorem 1.

**Proposition 1.** *Let  $Q$  be a non-singular integer ternary quadratic form of which  $(0, 1, 0)$  is a zero. Then for any  $\epsilon > 0$ , one has*

$$N(Q, B) = c_Q B + O_\epsilon \left( (BK_0)^{\frac{1}{2}} \log(BK_0) (|\Delta_Q|^{\frac{3}{2}} + |\Delta_Q|^{\frac{1}{2}} \langle Q \rangle) \langle Q \rangle^\epsilon \right),$$

for  $B \geq 2$ .

Let  $\Pi$  be the matrix

$$\Pi := \begin{pmatrix} b & e & 0 \\ -a & -d & -f \\ 0 & b & e \end{pmatrix}$$

and define the three binary quadratic forms  $q_1, q_2, q_3$  such that

$$(2.1) \quad \mathbf{q}(s, t) = \Pi \begin{pmatrix} s^2 \\ st \\ t^2 \end{pmatrix}$$

where  $\mathbf{q} = (q_1, q_2, q_3)^T$ . One can verify that  $\text{Det}(\Pi) = \Delta_Q$ , and that in particular the matrix  $\Pi$  is invertible. Hence one gets

$$(2.2) \quad \text{adj}(\Pi)\mathbf{q}(s, t) = \Delta_Q \begin{pmatrix} s^2 \\ st \\ t^2 \end{pmatrix}.$$

Notice that for

$$(2.3) \quad \begin{aligned} g(s, t) &:= as^2 + dst + ft^2, \\ L(s, t) &:= bs + et, \end{aligned}$$

one has

$$(2.4) \quad \begin{aligned} q_1(s, t) &= sL(s, t), \\ q_2(s, t) &= -g(s, t), \\ q_3(s, t) &= tL(s, t). \end{aligned}$$

For each integer  $n$ , let

$$(2.5) \quad \rho^*(n) := \#\{(s, t) \in (\mathbb{Z}/n\mathbb{Z})^2 : n|\mathbf{q}(s, t), \gcd(s, t, n) = 1\},$$

and note that  $\rho^*$  is a multiplicative function. Equations (2.4) imply that this expression can be simplified to

$$\rho^*(n) = \#\{(s, t) \in (\mathbb{Z}/n\mathbb{Z})^2 : n|(L(s, t), g(s, t)), \gcd(s, t, n) = 1\}.$$

**Lemma 1.** (1) *The function  $\rho^*$  is supported on the divisors of  $\Delta_Q$ .*

(2) *For each prime  $p$  and integer  $\nu \geq 0$ , we have*

$$\frac{\rho^*(p^\nu)}{p^\nu} \leq p^{\frac{v_p(\Delta_Q)}{2}}.$$

*Proof.* (1) Let  $p^\nu$  be such that  $\rho^*(p^\nu)$  is non-vanishing and let  $s, t$  be counted by  $\rho^*(p^\nu)$ . Considering (2.2) reduced (mod  $p^\nu$ ), we deduce that  $p^\nu$  divides both  $s^2\Delta_Q$  and  $t^2\Delta_Q$ . The fact that one of  $s, t$  is not divisible by  $p$ , implies that we must have  $p^\nu|\Delta_Q$ .

(2) We begin by proving that

$$(2.6) \quad \frac{\rho^*(p^\nu)}{p^\nu} \leq p^{\min\{v_p(b), v_p(e)\}}.$$

Let  $(s, t)$  be counted by  $\rho^*(p^n)$ . We may assume without loss of generality that  $v_p(b) \leq v_p(e)$ . In the case that  $n \leq v_p(b)$ , the trivial bound  $\rho^*(p^n) \leq p^{2n}$  proves (2.6). In the case that  $n > v_p(b)$ , we may write  $b = p^{v_p(b)}b', e = p^{v_p(e)}e'$ , such that  $p \nmid b'e'$ . Plugging these values into  $L(s, t) \equiv 0 \pmod{p^n}$ , yields  $b's \equiv -p^{v_p(e)-v_p(b)}e't \pmod{p^{n-v_p(b)}}$  and in particular  $p \nmid t$ . Hence the value of  $s/t \pmod{p^{n-v_p(b)}}$  is uniquely determined and can be lifted to at most  $p^{v_p(b)}$  values  $\pmod{p^n}$ , which proves (2.6) in all cases. To finish the proof, notice that the definition of the discriminant, given in the beginning of this section, implies that  $\gcd(b, e)^2 | \Delta_Q$ .  $\square$

We record a generalisation of Möbius inversion that will be used later.

**Lemma 2.** *Let  $\mathcal{I}$  be a finite subset of  $\mathbb{Z}^2$  and  $n$  a fixed integer. Then*

$$\begin{aligned} & \# \{(s, t) \in \mathcal{I} : \gcd(s, t) = 1\} \\ &= \sum_{\substack{m=1 \\ \gcd(m, n)=1}}^{\infty} \mu(m) \# \left\{ (s, t) \in \mathcal{I} : \begin{array}{l} \gcd(s, t, n) = 1, \\ m|s, m|t \end{array} \right\}. \end{aligned}$$

*Proof.* Define  $\mathbf{1}_{\mathcal{I}} : \mathbb{Z}^2 \rightarrow \{0, 1\}$  as the indicator function of  $\mathcal{I}$ . Möbius inversion gives

$$\sum_{\substack{\gcd(s, t, n)=1 \\ \gcd(s, t)=1}} \mathbf{1}_{\mathcal{I}}(s, t) = \sum_{m=1}^{\infty} \mu(m) \sum_{\substack{\gcd(s, t, n)=1 \\ m|s, m|t}} \mathbf{1}_{\mathcal{I}}(s, t).$$

Our assertion is proved upon noticing that only  $m$  coprime to  $n$  are taken into account in the summation.  $\square$

### 3. PARAMETRISATION OF THE CONIC

In this section, we begin by showing how the problem of counting points on conics can be rephrased using the parametrisation functions  $\mathbf{q}(s, t)$ . This will lead us to count primitive integer points in a region of  $\mathbb{R}^2$ .

Let

$$(3.1) \quad \mathcal{N}(Q, B) := \# \{(s, t) \in \mathbb{Z}_{\text{prim}}^2 : t > 0, \|\mathbf{q}(s, t)\| \leq \lambda B\},$$

where  $\lambda = \gcd(\mathbf{q}(s, t)) \in \mathbb{Z}$ .

**Lemma 3.** *One has  $N(Q, B) = \mathcal{N}(Q, B) + O(1)$ , where the implied constant is absolute.*

*Proof.* Let  $C \subset \mathbb{P}^2$  be the curve given by  $Q = 0$  and denote the point  $(0, 1, 0)$  of  $C$  by  $\xi$ . The tangent line to  $C$  through  $\xi$ , is given by

$$L_{\xi} := \{ez = bx\}.$$

Let  $\mathcal{L}$  be the set of projective lines in  $\mathbb{P}^2$  that pass through  $\xi$  and  $\mathcal{L}(\mathbb{Q})$  be the corresponding subset of lines that are defined over  $\mathbb{Q}$ . Define  $U \subset C$  as the open subset formed by deleting  $\xi$  from  $C$ . Letting  $\mathcal{U} := \mathcal{L} \setminus \{L_\xi\}$ , we note that the sets  $U(\mathbb{Q})$  and  $\mathcal{U}(\mathbb{Q})$  are in bijection.

The general element of  $\mathcal{L}(\mathbb{Q})$  is given by

$$L_{s,t} := \{sz = tx\}$$

for integer pairs  $(s, t)$  such that  $\gcd(s, t) = 1$ . The condition  $(s, t) \neq \frac{(b, e)}{\gcd(b, e)}$  ensures that we have a point in  $\mathcal{U}(\mathbb{Q})$ . One can ignore this, since the contribution of such  $s, t$  is  $O(1)$ . The bijection between lines with  $t > 0$  and  $t < 0$  allows us to consider the contribution coming from the former. The contribution of pairs  $(s, t)$  with  $t = 0$  is  $O(1)$  due to the condition  $\gcd(s, t) = 1$ .

One can make explicit the bijection of  $U(\mathbb{Q})$  and  $\mathcal{U}(\mathbb{Q})$  as follows. Recalling the definition of  $L, g$  in (2.3), a computation reveals that the line  $L_{s,t}$  intersects  $C$  in the point  $[x, y, z]$  if and only if  $z = 0$  or  $zg(s, t) + yL(s, t) = 0$ . In the former case, one gets the point  $\xi$ , which is to be ignored. In the latter case, we have

$$-g(s, t)xt = -g(s, t)sz = syL(s, t)t,$$

by the equation for  $L_{s,t}$ . The primitive integer vectors  $(x, y, z)$  represent a point in  $C(\mathbb{Q})$  if and only if

$$(x, y, z) = \pm(sL(s, t)/\lambda, -g(s, t)/\lambda, tL(s, t)/\lambda),$$

where  $\lambda = \gcd(sL(s, t), -g(s, t), tL(s, t))$ . Making use of (2.4) concludes the proof of the lemma.  $\square$

Let us define for any  $T \in \mathbb{R}_{\geq 1}$  and  $n, \sigma, \tau \in \mathbb{N}$ ,

$$(3.2) \quad M_{\sigma, \tau}^*(T, n) := \# \left\{ (s, t) \in \mathbb{Z}_{\text{prim}}^2 : \begin{array}{l} (s, t) \equiv (\sigma, \tau) \pmod{n}, \\ t > 0, \quad \|\mathbf{q}(s, t)\| \leq T \end{array} \right\}.$$

**Lemma 4.** *One has*

$$\mathcal{N}(Q, B) = \sum_{k\lambda | \Delta_Q} \mu(k) \sum_{\substack{(\sigma, \tau) \pmod{k\lambda} \\ k\lambda | (L(\sigma, \tau), g(\sigma, \tau))}}^* M_{\sigma, \tau}^*(B\lambda, k\lambda).$$

*Proof.* Any integer  $\lambda$  that appears in (3.1), satisfies  $\lambda | \mathbf{q}(s, t)$  for some coprime integers  $s, t$ , so part (1) of Lemma 1 implies that  $\lambda | \Delta_Q$ . One therefore gets

$$\mathcal{N}(Q, B) = \sum_{\lambda | \Delta_Q} \# \left\{ (s, t) \in \mathbb{Z}_{\text{prim}}^2 : \begin{array}{l} \lambda | \mathbf{q}(s, t), \quad \gcd(\frac{\mathbf{q}(s, t)}{\lambda}) = 1, \\ t > 0, \quad \|\mathbf{q}(s, t)\| \leq B\lambda \end{array} \right\}.$$

Using Lemma 2 with  $n = 1$ , gives

$$(3.3) \quad \mathcal{N}(Q, B) = \sum_{k\lambda | \Delta_Q} \mu(k) M^*(B\lambda, k\lambda),$$

where for any  $T \geq 1, n \in \mathbb{N}$ , we have defined

$$M^*(T, n) := \# \left\{ (s, t) \in \mathbb{Z}_{\text{prim}}^2 : \begin{array}{l} n | \mathbf{q}(s, t), \ t > 0, \\ \|\mathbf{q}(s, t)\| \leq T \end{array} \right\}.$$

Partitioning into congruence classes (mod  $n$ ), yields

$$(3.4) \quad M^*(T, n) = \sum_{\substack{(\sigma, \tau) \pmod{n} \\ n | (L(\sigma, \tau), g(\sigma, \tau))}}^* M_{\sigma, \tau}^*(T, n),$$

which when used along with (3.3), yields the proof of the lemma.  $\square$

#### 4. COUNTING LATTICE POINTS

The quantity appearing in (3.2) involves integer points  $(s, t)$  which are primitive. We will use Möbius inversion to deal with this condition. This will lead us to count integer points in a dilated region. In order to do so, one needs certain information on the behaviour of the region, which we proceed to do now.

Recall the definition (2.1). Denote by  $V$  the region

$$(4.1) \quad V := \{(s, t) \in \mathbb{R}^2 : t > 0, \|\mathbf{q}(s, t)\| \leq 1\}.$$

**Lemma 5.**  *$V$  is bounded and in particular, it is contained in the rectangle given by*

$$|s|, |t| \ll \langle Q \rangle \left( \frac{K_0}{|\Delta_Q|} \right)^{\frac{1}{2}}.$$

*In addition, the length of the boundary of  $V$  satisfies*

$$|\partial V| \ll \langle Q \rangle \left( \frac{K_0}{|\Delta_Q|} \right)^{\frac{1}{2}}.$$

*Proof.* For each  $(s, t) \in V$ , one gets from (2.2) that

$$|s|^2, |t|^2 \ll K_0 \|\text{adj}(\Pi)\|_{\infty} |\Delta_Q|^{-1}.$$

Using  $\|\text{adj}(\Pi)\|_{\infty} \ll \|\Pi\|^2$ , concludes the proof of the first asserted bound. Notice that the length of the part of a hyperbola or ellipse centered at the origin and which is contained in a circle centered at the origin with radius  $r$ , is bounded by  $O(r)$ . This observation concludes the proof of the lemma.  $\square$

Define for any  $T \in \mathbb{R}_{\geq 1}$  and  $n, \sigma, \tau \in \mathbb{N}$  such that  $\gcd(\sigma, \tau, n) = 1$ ,

$$(4.2) \quad M_{\sigma, \tau}(T, n) := \# \left\{ (s, t) \in \mathbb{Z}^2 : \begin{array}{l} (s, t) \equiv (\sigma, \tau) \pmod{n}, \\ t > 0, \|\mathbf{q}(s, t)\| \leq T \end{array} \right\}.$$

**Lemma 6.** *For any  $T, n, \sigma, \tau$  as above with  $\gcd(\sigma, \tau, n) = 1$  and  $n | \mathbf{q}(\sigma, \tau)$ , one has*

$$M_{\sigma, \tau}^*(T, n) = \sum_{\substack{1 \leq m \leq (2BK_0/n)^{\frac{1}{2}} \\ \gcd(m, n) = 1}} \mu(m) M_{\bar{m}\sigma, \bar{m}\tau} \left( \frac{T}{m^2}, n \right),$$

where  $\bar{m}$  denotes the inverse of  $m \pmod{n}$ .

*Proof.* The condition  $\|\mathbf{q}(s, t)\| \leq T$  implies by Lemma 5, that the number of  $(s, t)$  counted by  $M_{\sigma, \tau}^*(T, n)$  is finite. Therefore Lemma 2 may be applied to yield

$$M_{\sigma, \tau}^*(T, n) = \sum_{\substack{m=1 \\ \gcd(m, n)=1}}^{\infty} \mu(m) M_{\bar{m}\sigma, \bar{m}\tau} \left( \frac{T}{m^2}, n \right).$$

If  $m > (2K_0 T/n)^{\frac{1}{2}}$ , then each  $(s, t)$  taken into account by  $M_{\bar{m}\sigma, \bar{m}\tau} \left( \frac{T}{m^2}, n \right)$ , satisfies  $\|\mathbf{q}(s, t)\|_{\infty} < \frac{n}{2}$ . The assumptions on  $\sigma, \tau, n$ , imply that  $n|\mathbf{q}(s, t)|$  which is only possible if  $\mathbf{q}(s, t) = \mathbf{0}$ . Due to (2.2), one has  $t = 0$  which contradicts the definition of (4.2).  $\square$

Recall the definitions (4.1) and (4.2).

**Lemma 7.** *For any  $T, n, \sigma, \tau$  as above, we have*

$$M_{\sigma, \tau}(T, n) = \text{vol}(V) \frac{T}{n^2} + O \left( 1 + \frac{(K_0 T)^{\frac{1}{2}}}{n} \frac{\langle Q \rangle}{|\Delta_Q|^{\frac{1}{2}}} \right).$$

*Proof.* The quantity  $M_{\sigma, \tau}(T, n)$  equals the number of integer points in the region

$$\mathcal{R} := \frac{T^{\frac{1}{2}}}{n} V - \left( \frac{\sigma}{n}, \frac{\tau}{n} \right),$$

where  $V$  is defined in (4.1). We now make use of the following result taken from [Ste47]:

*Let  $\mathcal{R}$  be a compact subset of  $\mathbb{R}^2$  with a continuous piecewise differentiable boundary. Then the number of points with integer coordinates that lie inside  $\mathcal{R}$  is equal to*

$$\text{vol}(\mathcal{R}) + O(1 + |\partial \mathcal{R}|),$$

where  $|\partial \mathcal{R}|$  denotes the length of the boundary of  $\mathcal{R}$ .

In order to apply this result, notice that  $\text{vol}(\mathcal{R}) = \text{vol}(V) \frac{T}{n^2}$  and  $|\partial \mathcal{R}| = \frac{T^{\frac{1}{2}}}{n} |\partial V|$ , so that the lemma may be proved upon using the second bound of Lemma 5.  $\square$

## 5. THE ASYMPTOTIC FORMULA

We are now in possession of the required lemmata to show the validity of Proposition 1. Before proceeding to the proof we should remark that we shall show the asymptotic formula of Proposition 1 with a different constant in place of  $c_Q$ , and only in the next section the two constants will be proved to coincide.

Let us now define the new constant, which we denote by  $c'_Q$ . Recall the definitions (2.5) and (4.1). Let

$$(5.1) \quad \sigma'_{\infty} := \text{vol}(V)$$



and for any prime  $p$ , let

$$(5.2) \quad \sigma'_p := \left(1 - \frac{1}{p^2}\right) \left(1 + \frac{1}{(1 + \frac{1}{p})} \sum_{d \geq 1} \frac{\rho^*(p^d)}{p^d}\right).$$

We then define

$$c'_Q := \sigma'_\infty \prod_p \sigma'_p.$$

Notice that Lemma 7 implies that

$$(5.3) \quad \sigma'_\infty \ll \langle Q \rangle^2 \frac{K_0}{|\Delta_Q|}.$$

In light of Lemma 3, it suffices to prove Proposition 1 for  $\mathcal{N}(Q, B)$  in place of  $N(Q, B)$ . Combining Lemma 4 and Lemma 6, gives

$$\mathcal{N}(Q, B) = \sum_{k\lambda|\Delta_Q} \mu(k) \sum_{\substack{(\sigma, \tau) \pmod{k\lambda} \\ k\lambda|\mathbf{q}(\sigma, \tau)}}^* \sum_{\substack{m \leq (2BK_0/k)^{\frac{1}{2}} \\ \gcd(m, k\lambda)=1}} \mu(m) M_{\bar{m}\sigma, \bar{m}\tau} \left( \frac{B\lambda}{m^2}, k\lambda \right).$$

Now notice that for

$$\mathcal{L} := \frac{(K_0 B)^{\frac{1}{2}}}{k\lambda^{\frac{1}{2}}} \frac{\langle Q \rangle}{|\Delta_Q|^{\frac{1}{2}}},$$

(5.3) and Lemma 7 imply that

$$M_{\bar{m}\sigma, \bar{m}\tau} \left( \frac{B\lambda}{m^2}, k\lambda \right) = \begin{cases} \sigma'_\infty \frac{B}{m^2 k^2 \lambda} + O\left(\frac{\mathcal{L}}{m}\right) & \text{if } m \leq \mathcal{L} \\ O(1) & \text{otherwise.} \end{cases}$$

The contribution due to  $m > \mathcal{L}$  is therefore  $\ll_\epsilon (BK_0)^{\frac{1}{2}} \Delta_Q^{\frac{3}{2}} \langle Q \rangle^\epsilon$ . We have used the bound  $\tau_k(n) \ll_{k, \epsilon} n^\epsilon$  as well as  $\rho^*(d) \ll d |\Delta_Q|^{\frac{1}{2}}$ , which can be inferred from part (2) of Lemma 1. The contribution of the remaining  $m$  is

$$\begin{aligned} & \sigma'_\infty B \sum_{k\lambda|\Delta_Q} \frac{\mu(k) \rho^*(k\lambda)}{k^2 \lambda} \sum_{\substack{m \leq \mathcal{L} \\ \gcd(m, k\lambda)=1}} \frac{\mu(m)}{m^2} \\ & + O_\epsilon \left( (BK_0)^{\frac{1}{2}} (\log BK_0) \langle Q \rangle^{1+\epsilon} |\Delta_Q|^{\frac{1}{2}} \right). \end{aligned}$$

Extending the summation over  $m$  to infinity, the error introduced in the main term is  $\ll_\epsilon (BK_0)^{\frac{1}{2}} \langle Q \rangle^{1+\epsilon} \Delta_Q^{\frac{1}{2}}$ , where we have made use of (5.3). Finally notice that the identity

$$\sum_{k\lambda|\Delta_Q} \frac{\mu(k) \rho^*(k\lambda)}{k^2 \lambda} \sum_{\substack{m \in \mathbb{N} \\ \gcd(m, k\lambda)=1}} \frac{\mu(m)}{m^2} = \frac{1}{\zeta(2)} \sum_{d|\Delta_Q} \frac{\rho^*(d)}{d} \prod_{p|d} \frac{1}{1 + \frac{1}{p}}$$

shows that the leading constant is equal to  $c'_Q$  as desired.

## 6. THE LOCAL DENSITIES

In this section, we prove the remaining part of Proposition 1 by showing the equality of the local densities. This validates the Peyre prediction for the leading constant in the asymptotic formula of the proposition.

One should notice here that both of the quantities  $\sigma'_\infty$  and  $\sigma'_p$  for primes  $p$ , are related to the parametrising functions  $\mathbf{q}(s, t)$  rather than to the form  $Q$ , as is the case with the densities  $\sigma_\infty$  and  $\sigma_p$ . One might attempt to show the equality by explicitly computing each density but such an approach would entail extra labour. We will instead prove the equality indirectly, by parametrising the solutions locally. This can be thought of as following the proof of the asymptotic formula locally, instead of over  $\mathbb{Q}$ .

Recall the definitions (1.3) and (5.2).

**Lemma 8.** *For each prime  $p$ , one has  $\sigma'_p = \sigma_p$ .*

*Proof.* The proof consists of two parts. In the first part we find an alternative expression for the quantity  $\sigma'_p$  and in the second part we show that this expression is equal to  $\sigma_p$ . Throughout this proof we let  $v$  stand for  $v_p(\Delta_Q)$ . Recall that by part (1) of Lemma 1,  $\rho^*(p^d)$  is 0, unless  $0 \leq d \leq v$ .

Let for any  $0 \leq d \leq v$  and  $n \geq d$ ,

$$\rho^*(p^n, p^d) := \#\{(\sigma, \tau) \pmod{p^n} : p \nmid (\sigma, \tau), p^d \mid \mathbf{q}(\sigma, \tau)\}.$$

Each congruence  $(\sigma, \tau) \pmod{p^d}$  can be lifted to  $p^{2(n-d)}$  congruences  $\pmod{p^n}$  and hence,

$$(6.1) \quad \rho^*(p^n, p^d) = p^{2(n-d)} \rho^*(p^d).$$

Let for any  $0 \leq d \leq v$  and  $n \geq 1 + v$ ,

$$(6.2) \quad \rho_d^*(p^n) := \#\{(\sigma, \tau) \pmod{p^n} : p \nmid (\sigma, \tau), \gcd(\mathbf{q}(\sigma, \tau), p^n) = p^d\}.$$

Then for  $1 \leq d \leq v - 1$  and  $n \geq v$ , the observation

$$p^d \parallel \mathbf{q}(\sigma, \tau) \iff p^d \mid \mathbf{q}(\sigma, \tau) \text{ and } p^{d+1} \nmid \mathbf{q}(\sigma, \tau)$$

leads to

$$(6.3) \quad \rho_d^*(p^n) = \rho^*(p^n, p^d) - \rho^*(p^n, p^{d+1}).$$

Similar considerations show that

$$(6.4) \quad \begin{aligned} \rho_0^*(p^n) &= p^{2n} \left(1 - \frac{1}{p^2}\right) - \rho^*(p^n, p), \\ \rho_v^*(p^n) &= \rho^*(p^v) p^{2(n-v)}. \end{aligned}$$

Using (6.1)–(6.4), a telescopic sum computation reveals that

$$(6.5) \quad \sigma'_p = \lim_{n \rightarrow \infty} p^{-2n} \sum_{d \geq 0} p^d \rho_d^*(p^n).$$

We proceed to relate  $\rho_d^*(p^n)$  and  $N^*(p^n)$ , which appears in the definition of  $\sigma_p$ . Note that by (2.4) one has

$$\rho_d^*(p^n) = \#\{(\sigma, \tau) \pmod{p^n} : p \nmid (\sigma, \tau), \gcd(L(\sigma, \tau), g(\sigma, \tau), p^n) = p^d\}.$$

This implies that whenever  $(x, z)$  is counted by  $\rho_d^*(p^n)$ , then

$$g(x, z) \equiv p^d a \pmod{p^n} \text{ and } L(x, z) \equiv p^d b \pmod{p^n},$$

for some  $a, b$  with  $p \nmid (a, b)$ . Now notice that we may restate the equation  $Q(\mathbf{x}) = 0$  as

$$yL(x, z) = -g(x, z).$$

This shows that  $y$  is uniquely defined  $\pmod{p^{n-d}}$  as

$$y \equiv -\frac{a}{b} \pmod{p^{n-d}}.$$

Each such value can be lifted to  $p^d$  values of  $y \pmod{p^n}$  and therefore one has

$$(6.6) \quad p^d \rho_d^*(p^n) = N_d^*(p^n),$$

where we have defined

$$N_d^*(p^n) := \#\left\{ \mathbf{x} \pmod{p^n} : \begin{array}{l} Q(\mathbf{x}) \equiv 0 \pmod{p^n}, p \nmid \mathbf{x}, \\ \gcd(L(x, z), g(x, z), p^n) = p^d \end{array} \right\}.$$

Inserting (6.6) into (6.5), shows that  $\sigma'_p = \sigma_p$ , since one can partition  $N^*(p^n)$  according to the values of  $\gcd(L, g, p^n)$ .  $\square$

Recall the definitions (1.2) and (5.1).

**Lemma 9.** *One has  $\sigma'_\infty = \frac{1}{2}\sigma_\infty$ .*

*Proof.* We will use the method of Peyre [Pey95] to calculate the value of the archimedean density  $\sigma_\infty$ . We parametrise the points via the choice of variables  $x, z$ , for which the Leray form  $\omega_{\mathcal{L}}(\mathbf{x})$  is given by  $|L(x, z)|^{-1} dx dz$ , since

$$\frac{\partial Q}{\partial y} = L(x, z).$$

Both  $\mathbf{x}$  and  $-\mathbf{x}$  represent the same point in  $\mathbb{P}^2$ , which implies that

$$\sigma_\infty = \frac{1}{2} \int \int_{\{x, z \in \mathbb{R}^2 : \|(x, -\frac{g(x, z)}{L(x, z)}, z)\| \leq 1\}} |L(x, z)|^{-1} dx dz.$$

The Jacobian of the transformation  $(x, z) = (q_1(s, t), q_3(s, t))$ , is equal to  $2|L(s, t)|^2$ . We therefore see that the archimedean density becomes

$$\int \int_{\{s, t \in \mathbb{R}^2 : \|\mathbf{q}(s, t)\| \leq 1\}} 1 ds dt = 2\sigma'_\infty,$$

which proves our claim.  $\square$

## 7. THE PROOF OF THEOREM 1

In this section we complete the proof of Theorem 1. One should notice that Proposition 1 is a special case of Theorem 1 and we may thus attempt to prove it by adopting the approach we followed to prove Proposition 1. However the resulting local densities  $\sigma'_p$  are rather complicated, making it hard to match them up with the Hardy–Littlewood local densities  $\sigma_p$ .

To overcome this difficulty, we instead choose to transform the general form  $Q$  into one to which Proposition 1 applies. The next lemma shows that one can find a suitable transformation with the lowest possible height.

**Lemma 10.** *Let  $\mathbf{a} \in \mathbb{Z}_{\text{prim}}^3$ . Then there exists  $M \in SL_3(\mathbb{Z})$  whose second column is  $\mathbf{a}$  and whose entries have maximum modulus  $O(\|\mathbf{a}\|_\infty)$ .*

*Proof.* By renaming indices if needed, we may assume that

$$0 < |a_1| \leq |a_2| \leq |a_3|.$$

Let us notice that an integer solution to the equation  $\mathbf{a}^t \mathbf{y} = 1$  exists, owing to the coprimality of  $\mathbf{a}$ . The previous inequality implies that we can pick  $s, t \in \mathbb{Z}$  such that  $\max\{|y_3 - a_1 t|, |y_2 - a_1 s|\} \leq \frac{|a_1|}{2}$ . Then the integer vector

$$\mathbf{x} := \mathbf{y} + s(a_2, -a_1, 0) + t(a_3, 0, -a_1)$$

satisfies  $\mathbf{a}^t \mathbf{x} = 1$  and  $\|\mathbf{x}\|_\infty \ll \|\mathbf{a}\|_\infty$ .

We now let  $x'_i := \frac{x_i}{\gcd(x_1, x_2)}$ ,  $i = 1, 2$  so that  $\gcd(x'_1, x'_2) = 1$ . We know therefore that an integer solution  $(x, y)$  of  $x'_1 x + x'_2 y = x_3$  can be found. Considering  $y - tx'_1$  in place of  $y$  if needed, we can prove as previously that we can find  $(x, y)$  that satisfy the previous equation as well as  $\max\{|x|, |y|\} \ll \|\mathbf{x}\|$ . A direct calculation may then reveal that the matrix

$$M := \begin{pmatrix} x'_2 & a_1 & -x \\ -x'_1 & a_2 & -y \\ 0 & a_3 & \gcd(x_1, x_2) \end{pmatrix}$$

possesses the required properties.  $\square$

*Proof of Theorem 1.* It is given that the quadratic form  $Q$  possesses a rational zero. One can therefore find, using Cassels [Cas55], a non-trivial integer zero  $\boldsymbol{\xi} := (x_0, y_0, z_0) \in \mathbb{Z}_{\text{prim}}^3$  of  $Q$  such that  $\|\boldsymbol{\xi}\|_\infty \ll \langle Q \rangle$ . We now transform the form  $Q$  using  $\mathbf{a} = \boldsymbol{\xi}$  in the previous lemma. It provides an integer matrix  $M$  of determinant 1 and of size

$$(7.1) \quad \|M\|_\infty \ll \langle Q \rangle$$

such that the quadratic form  $Q'$  defined by

$$Q'(\mathbf{x}) := Q(M\mathbf{x}),$$

possesses the zero  $(0, 1, 0)$ . We define the norm given by

$$\|\mathbf{x}\|' := \|M\mathbf{x}\|$$

and notice that

$$\|Q'\| \ll \langle Q \rangle^3.$$

The fact that  $M$  is unimodular implies that the integer vector  $\mathbf{x}$  is primitive if and only if  $M\mathbf{x}$  is. It therefore follows that

$$N(Q, B) = N'(Q', B),$$

where the notation  $N'$  indicates a use of the norm  $\|\cdot\|'$ . The bound (7.1) shows that for  $K_1 := 1 + \sup_{\mathbf{x} \neq 0} \frac{\|\mathbf{x}\|_\infty}{\|\mathbf{x}\|'}$ , we have

$$K_1 \ll K_0 \langle Q \rangle^2,$$

where  $K_0$  is given by (1.5). Finally, notice that the discriminants of the quadratic forms remain invariant under the unimodular transformation  $M$ .

We are now in a position to apply Proposition 1 to the form  $Q'$ , with all involved quantities modified as indicated hitherto. The error term provided can be seen to be

$$\ll_\epsilon (BK_0)^{0.5} \log(BK_0) \langle Q \rangle^{\frac{11}{2} + \epsilon},$$

as a direct application of the preceeding inequalities. Recall the definition (1.2) and (1.3) of the local densities. It remains to show that they satisfy

$$\sigma_\infty(Q', \|\cdot\|') = \sigma_\infty(Q, \|\cdot\|)$$

and

$$\sigma_p(Q') = \sigma_p(Q)$$

for any prime  $p$ . The fact that the matrix  $M$  is invertible (mod  $p^n$ ) shows that  $N^*(Q, p^n) = N^*(Q', p^n)$  is valid, which when used in (1.3) proves the latter equality. The former is proved by performing the unimodular linear change of variables  $\mathbf{x} = M\mathbf{X}$  in (1.2). Hence

$$\int_{\substack{|Q(\mathbf{x})| \leq \epsilon \\ \|\mathbf{x}\| \leq 1}} 1 d\mathbf{x} = \int_{\substack{|Q'(\mathbf{X})| \leq \epsilon \\ \|\mathbf{X}\|' \leq 1}} 1 d\mathbf{X},$$

which finishes the proof of Theorem 1.

**Acknowledgements:** I would like to express my gratitude to my supervisor Tim Browning for suggesting the problem and for his valuable assistance during the course of the project.

## REFERENCES

- [BHB05] T. D. Browning and D. R. Heath-Brown, *Counting rational points on hypersurfaces*, J. Reine Angew. Math. **584** (2005), 83–115.
- [BVV12] T. D. Browning and K. Van Valckenborgh, *Sums of three squareful numbers*, Exp. Math. **21** (2012), no. 2, 204–211.
- [Cas55] J. W. S. Cassels, *Bounds for the least solutions of homogeneous quadratic equations*, Proc. Cambridge Philos. Soc. **51** (1955), 262–264.
- [CR03] J. E. Cremona and D. Rusin, *Efficient solution of rational conics*, Math. Comp. **72** (2003), no. 243, 1417–1441 (electronic).
- [FMT89] J. Franke, Y. I. Manin, and Y. Tschinkel, *Rational points of bounded height on Fano varieties*, Invent. Math. **95** (1989), no. 2, 421–435.
- [HB96] D. R. Heath-Brown, *A new form of the circle method, and its application to quadratic forms*, J. Reine Angew. Math. **481** (1996), 149–206.
- [Hoo68] C. Hooley, *On the Diophantine equation  $ax^2 + by^2 + cz^2 + 2fyz + 2gzx + 2hxy = 0$* , Arch. Math. (Basel) **19** (1968), 472–478.
- [Pey95] E. Peyre, *Hauteurs et mesures de Tamagawa sur les variétés de Fano*, Duke Math. J. **79** (1995), no. 1, 101–218.
- [Sim06] D. Simon, *Sur la paramétrisation des solutions des équations quadratiques*, J. Théor. Nombres Bordeaux **18** (2006), no. 1, 265–283.
- [Ste47] H. Steinhaus, *Sur un théorème de M. V. Jarník*, Colloquium Math. **1** (1947), 1–5.

SCHOOL OF MATHEMATICS, UNIVERSITY OF BRISTOL, BRISTOL, BS8 1TW,  
UNITED KINGDOM

*E-mail address:* efthymios.sofos@bristol.ac.uk